UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/050,764	01/18/2002	Thomas J. Walls	CIG-109	7742

28970 7590 04/03/2006

PILLSBURY WINTHROP SHAW PITTMAN LLP
1650 TYSONS BOULEVARD
MCLEAN, VA 22102

EXAMINER
CERVETTI, DAVID GARCIA

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 04/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

6

Office Action Summary	**Application No.** 10/050,764	**Applicant(s)** WALLS ET AL.	
	Examiner David G. Cervetti	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 January 2006*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 January 2002* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Applicant's arguments filed January 20, 2006, have been fully considered but they are not persuasive.

2. Claims 1-19 are pending and have been examined.

Response to Amendment

3. The objection to the drawings is withdrawn.

4. Regarding the arguments against the removal of the hyperlink or other browser executable code, Examiner submits a quote from MPEP 608.01:

> "Examiners must review patent applications to make certain that hyperlinks and other forms of browser-executable code, **especially commercial site URLs, are not included in a patent application**. >37 CFR 1.57(d) states that an incorporation by reference by hyperlink or other form of browser executable code is not permitted.< Examples of a hyperlink or a browser-executable code are a URL placed between these symbols "< >" and http:// followed by a URL address. When a patent application with embedded hyperlinks and/or other forms of browser-executable code issues as a patent (or is published as a patent application publication) and the patent document is placed on the USPTO web page, when the patent document is retrieved and viewed via a web browser, the URL is interpreted as a valid HTML code and it becomes a live web link. When a user clicks on the link with a mouse, the user will be transferred to another web page identified by the URL, if it exists, which could be a commercial web site. USPTO policy does not permit the USPTO to link to any commercial sites since the USPTO exercises no control over the organization, views or accuracy of the information contained on these outside sites." (emphasis added).

5. The following prior art has been used in this office action: Wagner et al. (NPL "A First Step Towards Automated Detection of Buffer Overrun Vulnerabilities", hereinafter Wagner), Viega et al. (NPL "ITS4: A Static Vulnerability Scanner for C and C++ Code", hereinafter Viega), Kolawa et al. (US patent 5,860,011, hereinafter Kolawa).

6. Applicant's interpretation of the prior art is noted.

7. Examiner submits that Wagner clearly teaches using a parser in the cited passages (figure 2, sections 1.1, 3.1, and 6-7), a further examination of the reference

teaches using a tree representing the source code (syntax) (section 3, and remaining of document) and Viega's teachings clearly teach creating and maintaining a vulnerability database (page 261, section 4.2). Applicant's arguments **are not persuasive.**

Specification

8. The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code (page 6, paragraph 17). Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01.

9. The disclosure is objected to because of the following informalities: twenty-none (page 27, paragraph 79). Appropriate correction is required.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

11. Claims 6-19 are rejected under 35 U.S.C. 102(b) as being anticipated by Kolawa.

Regarding claim 6, Kolawa teaches a vulnerability knowledge database (column 5, lines 1-57) comprising one or more classes of known software vulnerabilities (column 5, lines 1-57), a code parser that generates an abstract syntax tree from the software application (column 5, lines 58-67, column 6, lines 1-52); a vulnerability code analyzer that compares the abstract syntax tree the classes of known software vulnerabilities to identify a set of potential exploitable software vulnerabilities (column 6, lines 52-67, column 7, lines 1-67); and a static analysis tool that performs a static analysis of the set of potential exploitable software vulnerabilities wherein the static analysis is flow sensitive analysis of a list of constraints, and wherein the results of the static analysis comprise a set of exploitable software vulnerabilities (column 3, lines 43-67, column 4, lines 1-67, column 8, lines 1-55).

Regarding claim 7, Kolawa teaches a dynamic analysis tool that performs a dynamic analysis of the set of exploitable software vulnerabilities to identify one or more false positives in the set of exploitable software vulnerabilities, wherein the one or more false positives are discarded from the set of exploitable software vulnerabilities (column 3, lines 43-67, column 4, lines 1-67).

Regarding claim 8, Kolawa teaches wherein the dynamic analysis tool executes the set of potential exploitable software vulnerabilities with a maximal number of testing configurations (column 4, lines 1-67, column 5, lines 1-67).

Regarding claim 9, Kolawa teaches wherein the vulnerability knowledge database is expandable (column 5, lines 1-57).

Regarding claim 10, Kolawa teaches a user interface that enables a user to enter an additional known software vulnerability to the vulnerability knowledge database (column 5, lines 1-57).

Regarding claim 12, Kolawa teaches a vulnerability knowledge database (column 5, lines 1-57) comprising one or more classes of known software vulnerabilities (column 5, lines 1-57); a code parser that generates an abstract syntax tree from the software application (column 5, lines 58-67, column 6, lines 1-52); a vulnerability code analyzer that compares the abstract syntax tree the classes of known software vulnerabilities to identify a set of potential exploitable software vulnerabilities (column 6, lines 52-67, column 7, lines 1-67); a user interface that presents the set of potential exploitable software vulnerabilities to a user and enables the user to select one or more potential exploitable software vulnerabilities from the set of potential exploitable software vulnerabilities (column 2, lines 46-67, column 3, lines 1-25, column 3, lines 43-67, column 4, lines 1-67); and a static analysis tool that performs a static analysis of the selected ones of the set of potential exploitable software vulnerabilities wherein the static analysis is flow sensitive analysis of a list of constraints, and wherein the results of the static analysis comprise a set of exploitable software vulnerabilities (column 3, lines 43-67, column 4, lines 1-67, column 8, lines 1-55).

Regarding claim 13, Kolawa teaches a dynamic analysis tool, wherein the user interface presents the set of exploitable software vulnerabilities and enables the selection of one or more of the exploitable software vulnerabilities from the set of exploitable software vulnerabilities, and wherein the dynamic analysis tool performs a dynamic analysis of the selected ones of the set of exploitable software vulnerabilities to identify one or more false positives in the set of exploitable software vulnerabilities, wherein the one or more false positives are discarded from the set of exploitable software vulnerabilities (column 3, lines 43-67, column 4, lines 1-67).

Regarding claim 14, Kolawa teaches wherein the dynamic analysis tool executes the selected ones of the set of potential exploitable software vulnerabilities with a maximal number of testing configurations (column 4, lines 1-67, column 5, lines 1-67).

Regarding claim 15, Kolawa teaches a dynamic analysis tool that performs a dynamic analysis of the set of exploitable software vulnerabilities to identify one or more false positives in the set of exploitable software vulnerabilities, wherein the one or more false positives are discarded from the set of exploitable software vulnerabilities (column 3, lines 43-67, column 4, lines 1-67).

Regarding claim 16, Kolawa teaches wherein the dynamic analysis tool executes the set of potential exploitable software vulnerabilities with a maximal number of testing configurations (column 4, lines 1-67, column 5, lines 1-67).

Regarding claim 17, Kolawa teaches wherein the vulnerability knowledge database is expandable (column 5, lines 1-57).

Regarding claim 18, Kolawa teaches wherein the user interface enables the user to enter an additional known software vulnerability to the vulnerability knowledge database (column 5, lines 1-57).

Regarding claims 11 and 19, Kolawa teaches wherein the set of exploitable software vulnerabilities comprises one or more of a security vulnerability, a safety vulnerability, or a reliability vulnerability (column 5, lines 1-57).

Claim Rejections - 35 USC § 103

12. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

13. Claims 1 and 4-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wagner, and further in view of Viega.

Regarding claim 1, Wagner teaches applying a code parser to the software application to generate an abstract syntax tree (figure 2); comparing the abstract syntax tree and the classes of known software vulnerabilities to identify a set of potential exploitable software vulnerabilities (Section I); and performing a static analysis of the set of potential exploitable software vulnerabilities wherein the static analysis is flow sensitive analysis of a list of constraints, and wherein the results of the static analysis comprise a set of exploitable software vulnerabilities (Sections 1.1, 3.1, and 6-7). Wagner teaches the use of a vulnerability database (section 1), but do not expressly disclose creating a vulnerability knowledge database comprising one or more classes of known software vulnerabilities. However, Viega teaches creating a vulnerability knowledge database comprising one or more classes of known software vulnerabilities (pages 258-263). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the vulnerability database of Viega with the system of Wagner. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use a database of vulnerabilities to check source code against it (Viega, page 261).

Regarding claim 4, the combination of Wagner and Viega teaches wherein the vulnerability knowledge database is expandable (Viega, pages 259-266).

Regarding claim 5, the combination of Wagner and Viega teaches wherein the set of exploitable software vulnerabilities comprises one or more of a security vulnerability, a safety vulnerability, or a reliability vulnerability (Viega, pages 259-266).

14. Claims 2-3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wagner and Viega, and further in view of Kolawa.

Regarding claim 2, the combination of Wagner and Viega does not expressly disclose dynamic analysis. However, Kolawa teaches performing a dynamic analysis of the set of exploitable software vulnerabilities to identify one or more false positives in the set of exploitable software vulnerabilities; and discarding the one or more false positives from the set of exploitable software vulnerabilities (column 3, lines 43-67, column 4, lines 1-67).

Regarding claim 3, the combination of Wagner, Viega, and Kolawa teaches wherein performing the dynamic analysis comprises executing the set of potential exploitable software vulnerabilities with a maximal number of testing configurations (Kolawa, column 4, lines 1-67, column 5, lines 1-67).

Conclusion

15. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

17. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

18. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DGC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100